SIMULACIÓ D'UN ATAC DE PHISHING

Treball de Fi de Grau

Presentat a

l'Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona

Universitat Politècnica de Catalunya

per

Xavier Medina Bosch

En compliment parcial dels requisits pel grau en

ENGINYERIA DE TECNOLOGIES I SERVEIS DE TELECOMUNICACIÓ

MENCIÓ EN SISTEMES TELEMÀTICS

Tutor: Oscar Esparza Martín

Barcelona, Gener 2019

Abstract

Phishing is a cyberattack which is very common in society, in professional areas as well as personal field. A large part of the population is susceptible to being a victim of this threat due to its propagation vector.

The objective of this project is to show the realization of a phishing attack, as well as carry out the task of raising awareness in society and cope with the emerging innovations.

The project consists of two big parts. In the first one, this threat is contextualized and its characteristics are explained. In the second one, it is performed a simulation of a phishing attack in a virtualized environment, where several variants are shown from the point of view of the attacker as well as the victim one.

Resum

El phishing és un atac cibernètic molt estès a la societat, tant en l'àmbit professional com particular. Donats els vectors de propagació, gran part de la població és susceptible a ser-ne víctima. Per contra, es manifesta un elevat desconeixement en els usuaris dels serveis relacionats.

L'objectiu d'aquest treball és mostrar la realització d'un atac de phishing, així com exercir la tasca de conscienciació a la societat i fer front a les innovacions que estan sorgint.

El projecte consta dos grans blocs. En el primer es contextualitza aquesta amenaça i se n'expliquen les principals característiques. En el segon es realitza una simulació d'un atac de phishing en un entorn virtualitzat, on es mostren diverses variants tant des del punt de vista de l'atacant com de la víctima.

Resumen

El phishing es un ataque cibernético muy extendido en la sociedad, tanto en el ámbito profesional como particular. Dados los vectores de propagación, gran parte de la población es susceptible a ser víctima. En cambio, se manifiesta un elevado desconocimiento en los usuarios de los servicios relacionados.

El objetivo de este trabajo es mostrar la realización de un ataque de phishing, así como ejercer la tarea de concienciación a la sociedad y afrontar las innovaciones que están surgiendo.

El proyecto consta de dos grandes bloques. En el primero se contextualiza esta amenaza y se explican sus principales características. En el segundo se realiza una simulación de un ataque de phishing en un entorno virtualizado, donde se muestran distintas variantes tanto desde el punto de vista del atacante como de la víctima.

Agraïments

Vull mostrar el meu agraïment als meus pares, Carmen i Jesús, perquè sense ells no hagués estat possible. A la Marina per recolzar-me i ajudar-me en tot moment. A la resta de família pel seu suport. Als companys de feina per guiar-me i aconsellar-me.

Moltes gràcies a tots.

Historial de revisions i registre d'aprovacions

Revisió	Data	Propòsit
0	29/12/2018	Creació del document
1	02/01/2019	Revisió del document
2	08/01/2019	Revisió del document
3	15/01/2019	Revisió del document
4	16/01/2019	Revisió del document
5	18/01/2019	Revisió del document
6	19/01/2019	Revisió del document
7	20/01/2019	Revisió del document
8	24/01/2019	Revisió del document

LLSITA DE DISTRIBUCIÓ DEL DOCUMENT

Nom	Correu electrònic
Xavier Medina Bosch	xavier.medina.bosch@alu-etsetb.upc.edu
Oscar Esparza Martin	oesparza@entel.upc.edu

Escrit per:		Revisat i aprovat per:	
Data	29/12/2018	Data	24/01/2019
Nom	Xavier Medina Bosch	Nom	Oscar Esparza Martin
Posició	Autor del projecte	Posició	Supervisor del projecte

Taula de continguts

Llista de Figures

1. Introducció

1.1. Objectius

L'objectiu principal d'aquest projecte és realitzar tres atacs de phishing que reflecteixin l'evolució d'aquesta amenaça. El primer és el tipus més habitual, el segon incorpora un fitxer adjunt que trenca amb l'estereotip augmentant el nombre de víctimes i el tercer és el més innovador, el qual entrega *malware*.

Els propòsits d'aquestes simulacions són:

- Mostrar els passos que conformen aquest atac, des de la seva creació fins al tractament de les dades proporcionades per la víctima.
- Exposar les tecnologies necessàries per a la seva creació.
- Mostrar les variants més comunes i les més innovadores.

Addicionalment s'expliquen les classificacions, les tècniques de detecció, classificació i els procediments que fan servir els professionals en ciberseguretat, tan en l'atac com en la defensa.

1.2. Requeriments i especificacions

Requeriments del projecte:

- Automatització d'enviament de correus electrònics massius
- Enginyeria Social
- Gestió de les dades de les víctimes

Especificacions del projecte:

- Definició de la metodologia
  - Tom's Planner Gantt
  - Lucidchart
- Llenguatges de programació
  - Python
  - HTML
  - PHP
- Sistemes
  - Apache2
  - MySQL
  - Ubuntu Linux
  - Metasploit Kali Linux

2. Estat de l'art del projecte

2.1. Enginyeria Social

L'enginyeria social [1] és el conjunt de tècniques o mètodes emprats per obtenir, de manera fraudulenta, informació confidencial de l'usuari. Aquesta branca no aprofita les vulnerabilitats de software si no la manipulació de les persones. Les tècniques més utilitzades per tal d'enganyar la gent són:

- **Urgència**: La víctima actuarà de manera més ràpida i no hi reflexionarà amb tanta profunditat. Un exemple comú és informar la víctima que la contrasenya del seu compte és pròxima a expirar, fent-li canviar el més aviat possible.
- **Confiança**: Provoca que la persona atacada disminueixi les defenses i es fiï amb més facilitat. Per exemple, en una trucada telefònica es demana facilitar el nombre de factura de la companyia elèctrica. La víctima l'entregarà abans si l'atacant proporciona un identificació i nom suplantats, si proporciona dades de la víctima per verificar l'autenticitat o si utilitza un to relaxat i afable.
- **Autoritat**: Fer-se passar per una persona de rang superior fa que la víctima tendeixi a proporcionar més fàcilment les dades perquè suposadament les necessita. Si el cap demana un informe a un treballador el qual conté informació confidencial, aquest el facilitarà amb major probabilitat que a un altre company del seu equip.
- **Validació social**: Es busca que la víctima rebi el reconeixement i l'aprovació per part del delinqüent fent-la sentir realitzada. Pot ser el cas en què un company demani les credencials a un altre amb el pretext de falta de permisos o bloqueig del compte i, per tal de sentir-se acceptat o pretendre ser educat, les hi proporcioni.

2.2. Phishing

2.2.1. Definició

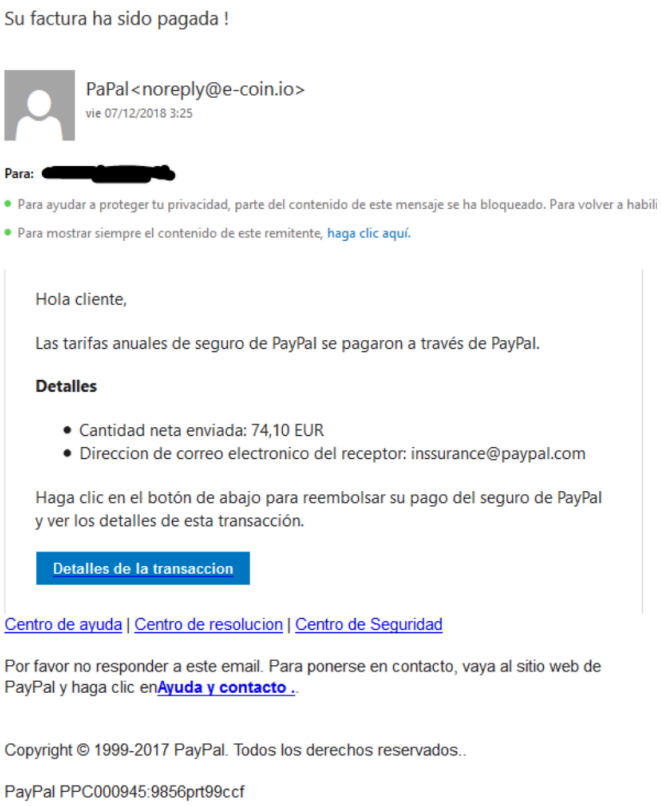
El phishing [2][3] és un atac d'enginyeria social l'objectiu del qual és la sostracció de dades de caràcter personal. Es propaga per mitjà de diversos actors com poden ser missatges SMS (*Smishing*), trucades telefòniques (*Vishing*), pàgines web que simulen una entitat, missatgeria instantània o, el més comú, el correu electrònic.

Els objectius més comuns són: dades d'accés a pàgines web com nom d'usuari, correu i contrasenya, DNI, targetes bancàries o part d'elles i números de telèfon.

En la majoria de casos, el ciberdelinqüent té més d'un camí per assolir l'objectiu. Sol·licitarà les dades que més li convinguin depenent del servei al qual suplanti. A l'apartat "2.PHISHING" de l'apèndix G es mostra un exemple pràctic.

El *phisher*, nom amb el qual es coneix l'actor que realitza aquest tipus d'atac, podrà utilitzar aquestes dades per accedir a diversos serveis de la víctima. Hi ha un ampli ventall de possibilitats. Les més comunes són les següents:

- **Compte bancari**: permet realitzar transferències i compres.
- **Correu electrònic**: es pot utilitzar per a múltiples objectius: obtenir informació de correus, cites del calendari o contactes emmagatzemats, fer-se passar per la persona afectada. Fins i tot pot ser emprat per canviar la contrasenya d'altres serveis.
- **Xarxes socials**: poden arribar a proporcionar informació personal tan de la víctima com d'altres usuaris, creant un perfil social dels gustos, preferències, ubicacions, relacions i altres dades que es poden utilitzar en contra d'elles.


Su factura ha sido pagada !

PaPal<noreply@e-coin.io>
vie 07/12/2018 3:25

Para: [redacted]

Para ayudar a proteger tu privacidad, parte del contenido de este mensaje se ha bloqueado. Para volver a habili

Para mostrar siempre el contenido de este remitente, haga clic aquí.

Hola cliente,

Las tarifas anuales de seguro de PayPal se pagaron a través de PayPal.

Detalles

- Cantidad neta enviada: 74,10 EUR
- Direccion de correo electronico del receptor: inssurance@paypal.com

Haga clic en el botón de abajo para reembolsar su pago del seguro de PayPal y ver los detalles de esta transacción.

Detalles de la transaccion

Centro de ayuda | Centro de resolucion | Centro de Seguridad

Por favor no responder a este email. Para ponerse en contacto, vaya al sitio web de PayPal y haga clic enAyuda y contacto .

Copyright © 1999-2017 PayPal. Todos los derechos reservados..

PayPal PPC000945:9856prt99ccf

Figura 1: Cas real de correu electrònic de phishing.

2.2.2. Spear Phishing

El *Spear Phishing* [4] és una variant del phishing la qual es diferencia per anar dirigida a persones, organitzacions o empreses específiques. Sovint inclouen *malware*, ja sigui adjunt al propi correu o amb un enllaç a una pàgina web on s'allotgi. D'aquesta manera es pretén infectar l'equip de la víctima per tenir accés a la informació que aquest contingui i també la d'altres equips de la xarxa.

La principal font on el criminal pot recollir informació a l'hora de definir el *target* de l'atac són les xarxes socials com Facebook, Twitter o Instagram. Cada cop més persones creen perfils on hi pengen informació personal, ja sigui de manera directa o indirecta. Fent un recull de la informació que un usuari ha dipositat en diverses d'elles, es pot crear un perfil de la persona i assignar-lo a un grup al qual es llançarà un atac dirigit.

En conclusió, el *Spear Phishing* es dirigeix a un públic concret i reduït, característica que disminueix la probabilitat que l'objectiu hi caigui si ho comparem amb el phishing tradicional. Tanmateix, els missatges contenen més detalls relacionats amb la persona en qüestió, la qual cosa els fa més creïbles que els genèrics de l'atac convencional, augmentant-ne la probabilitat d'èxit. Addicionalment cal tenir en compte els adjunts maliciosos els quals tenen un impacte encara major per a la pesca d'informació.

2.2.3. Whaling Phishing

Quan el missatge va dirigit a als alts càrrecs d'una organització, l'atac pren el nom de *Whaling Phishing* [5]. Són persones involucrades en decisions d'alt nivell que tenen accés a finances i informació corporativa. Sovint s'anomena aquest col·lectiu amb l'expressió col·loquial "peixos grossos", a partir del qual s'ha inspirat el nom de l'amenaça. El *whaling* involucra més enginyeria social que accions tecnològiques complexes al ser molt més específic. Se cerca més informació d'una persona concreta amb l'objectiu de crear un perfil el més complet possible i poder elaborar un email detallat i creïble.

També es consideren els casos on el remitent del missatge es fa passar pel directiu i es dirigeix a treballadors o clients sol·licitant informació d'interès. Aquests faciliten les dades pensant que són urgentment necessàries. A l'apartat "2.2 WHALING PHISHING" de l'apèndix G es mostra un cas real.

2.2.4. Detecció de phishing

El Phishing és un tipus d'atac dirigit a l'usuari on els paràmetres emprats són diferents en cada cas: dades dels correus, enllaços a webs fraudulentes, dades a robar, passos que el formen, vector d'atac i altres factors. Aquest fet implica la impossibilitat a l'hora de detectar, aturar i reportar un incident per complet de manera automatitzada.

La solució més adequada és prevenir les persones. Una bona educació augmenta la probabilitat d'identificació d'un phishing. Les característiques més freqüents [6] són les següents:

- **Faltes d'ortografia**: Sovint els phishings en contenen moltes ja que es realitzen en països estrangers utilitzant traductors.
- **URL falsa**: La URL del *hipervincle* del missatge no és la lícita del servei en qüestió. Hi ha casos en què és semblant, altres en què el domini és totalment diferent i fins i tot hi ha casos on es mostra directament la IP del servidor.
- **HTTPS**: És la versió segura del protocol HTTP i cada vegada més utilitzada. Està basada en connexions mitjançant canals xifrats mitjançant certificats SSL/TLS. Proporciona confidencialitat evitant escoltes intermèdies entre l'origen i el destí com atacs *man-in-the-middle* i *eavesdropping*.
- **URL escurçada**: Sovint s'abreuja la URL per dos motius: no fer visible el domini, ja que és fals, i mostrar un *hipervincle* amb HTTPS, ja que el servei d'escurçament sí que ho és a diferència de la web de phishing.
- **Referer**: Freqüentment l'últim pas d'un phishing és redirigir a la pàgina web real per fer creure que hi ha hagut un error després de proporcionar les dades i no sospitar de l'engany. Si una empresa detecta que s'ha a la seva web mitjançant una redirecció, és probable que s'hagi produït un phishing.
- **Spoofing**: Consisteix a modificar les capçaleres SMTP del correu mostrant un remitent diferent a l'adreça real des d'on s'ha enviat i que sigui similar al del servei suplantat.

- **Destinataris a CCO**: En casos de phishings massius és comú afegir els destinataris a l'apartat CCO (*Carbon Copy Ocult*) del correu per no mostrar que s'envia a més adreces i amagar la gran quantitat de destins.

Algunes empreses creen eines que analitzen els *emails* tenint en compte aquestes característiques entre moltes altres. A partir dels resultats, basant-se en mètodes de puntuació o *scoring,* poden determinar la probabilitat que es tracti d'un atac de phishing.

2.2.4.1. Clausura

Quan el departament de ciberseguretat d'una empresa detecta un phishing, el seu objectiu és clausurar-lo per evitar afectació als seus clients. Per fer-ho, es reporta el cas a l'operador de xarxa i aquest duu a terme un seguit de comprovacions i procediments els quals s'expliquen a l'apartat "3.1 PROCEDIMENT DE CLAUSURA D'UN CAS DE PHISHING" de l'apèndix G.

2.2.5. Classificació de phishing

2.2.5.1. Campanya

Es considera una campanya al conjunt d'atacs amb les mateixes característiques o variacions d'aquestes: objectiu, assumpte, remitent, fitxer adjunt, pàgina web fraudulenta i altres factors que hi actuïn.

2.2.5.2. Kit

Els kits són plantilles utilitzades per llançar atacs de phishing. Comunament són escrits per un agent i posteriorment venuts a tercers, els quals duran a terme l'atac. Poden ser usats per persones amb baix nivell tècnic.

Cada autor realitza el seu kit d'una manera pròpia. El llenguatge de programació escollit, les variables emprades, el nombre de passos, la manera de tractar les dades sostretes, etc. Els professionals estudien el codi font, redireccions, emmagatzematge de dades i demés característiques, classifiquen els kits i els inclouen a un inventari. Així, nous casos amb el mateix kit seran detectats de manera més eficient. També serveixen per observar les tendències dels atacs i crear nous mètodes de detecció.

Aquesta tècnica permet que, en cas que una pàgina fraudulenta sigui detectada i clausurada, es pugui reutilitzar el mateix kit creant una nova pàgina o allotjant-lo en un nou servidor.

2.2.6. Obtenció de contactes

Hi ha diverses maneres per les qual el phisher pot obtenir contactes [7], ja siguin adreces de correu o telèfons. Es poden comprar bases de dades a empreses, consultar-ne de genèriques i es donen casos de robatoris i mercats negres. També es poden adquirir a *blogs*, xarxes socials i enquestes. Addicionalment existeixen softwares que escanegen internet buscant contactes.

2.3. Email

El correu electrònic [8], conegut també com *email* (de l'anglès *electronic mail*) és un sistema de comunicació per missatgeria a través de xarxes electròniques. El client de correu electrònic del remitent obre una connexió amb el servidor de email a través del port TCP 25, on diposita el missatge per a que aquest l'enviï als destinataris. El missatge viatja a través de la xarxa per diversos servidors fins a arribar al servidor destí, el qual entrega el correu al client destí. En aquest procés hi participen tres grans protocols de transmissió de missatges: El primer és SMTP [9][10][15] que actua des de la primera connexió del client amb el servidor de correu fins que el missatge arriba al servidor destí. Els altres són IMAP [9][16] i POP3 [9][17] que s'encarreguen d'entregar el missatge al client destí segons convingui.

És el vector més utilitzat en els atacs de phishing per la gran quantitat d'usuaris i perquè es pot accedir des de molts tipus de dispositius. Per aquest motiu s'han creat filtres antiphishing i antispam com SPF [11], DKIM [12] i DMARC [13], explicats a l'apartat "3.2 ESTÀNDARDS DE VALIDACIÓ" de l'apèndix F.

El procés de transmissió d'un correu electrònic és el següent:

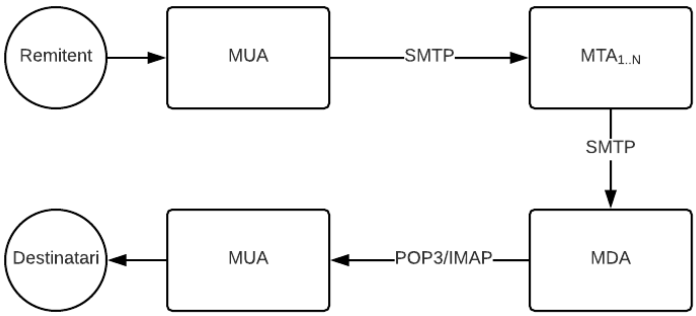


Figura 2: Procés de transmissió d'un correu electrònic.

- **MUA** [14] (*Mail User Agent*): Software mitjançant el qual l'usuari confecciona i gestiona els correus electrònics. Quan el software és instal·lat al sistema s'anomena client de correu electrònic, mentre que si es tracta d'una interfície web aleshores s'anomena *webmail*.
- **MTA** [14] (*Mail Transfer Agent*): Servidors encarregats de transmetre el correu per la xarxa fins a arribar al servidor destí. També són anomenats servidors SMTP pel protocol que utilitzen per a la transmissió.
- **MDA** [14] (*Mail Delivery Agent*): Servidor que rep el missatge i l'emmagatzema a l'espera de ser acceptat pel receptor. Utilitza principalment dos protocols en la transmissió amb el MUA destí: POP3 i IMAP.

2.3.1. Protocols

2.3.1.1. SMTP

El protocol SMTP, acrònim de *Simple Mail Transfer Protocol*, és un protocol de xarxa que s'encarrega d'intercanviar missatges de correu electrònic seguint una estructura client-servidor descrit a la RFC 5321. És senzill, ja que està basat en text codificat en ASCII, i útil a la vegada. S'intercanvien línies seguint un ordre estricte, on el client emet una comana i el servidor retorna una resposta. Les respostes estan formades per un nombre i un text descriptiu del codi retornat: 2XX resposta afirmativa, 3XX resposta temporal afirmativa, 4XX resposta d'error i espera fins que es repeteixi la instrucció i 5XX resposta d'error.

A l'apartat "3.SMTP" de l'apèndix F es mostra un exemple de sessió SMTP i un exemple de les capçaleres d'un correu.

2.3.1.2. POP3 i IMAP

La transmissió d'un missatge de correu electrònic des del servidor de email al client del destinatari es duu a terme per mitjà del protocol POP3 o IMAP.

El protocol POP3, sigles de *Post Office Protocol version 3*, s'especifica a la RFC 1939. El seu funcionament és el següent:

1. El client es connecta al servidor pel port 110 o, per a connexions amb SSL/TLS, pel port 995.
2. Recupera els emails.
3. Elimina les còpies dels missatges emmagatzemades al servidor.
4. Tanca la connexió amb el servidor.

Segons l'ús que se'n vulgui fer, es pot configurar per tal que segueixi emmagatzemant les còpies dels correus al servidor.

El protocol IMAP, sigles de *Internet Message Access Protocol*, s'especifica a la RFC 3501. El seu funcionament és el següent:

1. El client es connecta al servidor pel port 143 o, per a connexions amb SSL/TLS, pel port 993.
2. Recupera els emails.
3. Manté la connexió fins que es tanca l'aplicació del client i descarrega els missatges sobre demanda.

Permet agrupar els missatges i arxivar-los en carpetes. Conté marcadors per indicar si un missatge ha estat llegit, eliminat o respost. Fins i tot és capaç de realitzar cerques a les bústies del servidor. Addicionalment, les còpies dels correus no són eliminades del servidor.

Donat que POP3 elimina les còpies dels missatges, permetrà disposar d'un servidor amb menys capacitat d'emmagatzematge. A més a més, donat que els missatges s'emmagatzemaran localment, es pot afirmar que existeix major privacitat. Addicionalment, és més simple d'implementar i consumeix menys recursos computacionals. D'altra banda, IMAP permet accedir als correus electrònics simultàniament des de diversos dispositius, ja que s'emmagatzema una còpia d'aquests

al servidor. A més a més, si es realitza una acció sobre un missatge des d'un dispositiu, ja sigui eliminar, reenviar moure, etc. també s'aplicarà l'acció sobre els altres.

2.4. Altres projectes

El phishing ha estat tema d'altres treballs de fi de grau. En alguns d'ells com a matèria principal i en altres, relacionada amb la principal.

En el projecte "El Phishing" [23] descriu aquest atac, explica les fases que el composa, com protegir-se i altres característiques a més de classificar-los. També exposa l'impacte econòmic i social d'aquesta amenaça. Finalment exposa alguns exemples. L'enfocament d'aquest és més social, ensenyant fins i tot algun apartat referent al codi penal, i es basa en explicacions teòriques. No realitza cap exemple pràctic

Una altra tesi que tracta aquest tema rep el nom "Análisis de Métodos de Ataques de Phishing" [24]. Se centra més en les xarxes socials i els serveis de missatgeria instantània. Es basa en situacions reals les quals analitza i en treu conclusions. Realitza un script a mode d'exemple pràctic en el qual sol·licita les dades de Facebook. Allotja el web phishing a un servei de *hosting* des del qual gestiona les dades.

Per últim, un altre treball basat en aquest atac és "Implementació d'un algoritme de detecció de phishing" [25]. Donada la confidencialitat, no ha pogut ser analitzat en detall. No obstant, està enfocat en la detecció de phishings. Per tant, se centra en el punt de vista del defensor de l'amenaça amb l'objectiu d'evitar que es produeixi afectació en un atac.

La principal diferència respecte d'aquest projecte és que en cap d'ells s'ha realitzat un atac complet que comprengui totes les fases, des del disseny fins al tractament de les dades sostretes passant per la implementació del vector d'atac, la pàgina web i l'obtenció de les credencials. Tampoc s'ha analitzat cap estadística basada en preguntes a persones de primera mà a través d'una enquesta, no s'han tractat les capçaleres SMTP ni s'han explicat els estàndards de validació. Addicionalment, en aquest treball es tracta el funcionament de la transmissió d'un correu electrònic i els sistemes antiphishing i antispam dels quals aquest disposa.

2.5. Eines de creació de phishing

Existeixen eines de creació de phishing automàtiques, és a dir, només cal indicar certs paràmetres i et crea la pàgina falsa. A continuació s'expliquen les més utilitzades recentment:

Una d'elles es troba al sistema operatiu Kali Linux [18] , anomenada **setooklit** [19], dins l'apartat d'enginyeria social i s'executa des del terminal. Permet diferents vectors d'atac web, un d'ells el phishing. Es poden escollir les credencials a sostreure entre múltiples opcions. Cal introduir la IP de la màquina i la URL del site a falsificar. Si el reconeix, crea una pàgina molt semblant a la IP indicada. El programa manté un procés esperant rebre les credencials introduïdes, les quals es poden consultar des del mateix terminal o des d'un fitxer creat automàticament.

Una altra de les més utilitzades és **SocialFish** [20], també de Kali Linux. Disposa de 7 plantilles: Facebook, Google, LinkedIn, Twitter, Stackoverflow, Wordpress i GitHub. Totes elles tenen un gran nombre d'usuaris i contenen informació personal i, per tant, molt valuosa i desitjada pels cibercriminals. Requereix de Python [21] 2.7, biblioteques Python per realitzar peticions Wget, PHP [22] i permisos de *root*. El funcionament és força semblant al programa anterior: després d'instal·lar-lo, s'executa, s'escull el recurs a clonar, genera un domini on el qual demana un altre cop la pàgina víctima i altres paràmetres i, finalment, genera un phishing web. El principal inconvenient és que el *site* generat no és igual que el real, fet que fa disminuir la probabilitat d'èxit en l'atac.

Aquestes eines generen un atac eficaç, ja que generen la web de phishing, però no eficient. Això és degut a que cal configurar l'entorn (LAMP), cal definir un vector d'atac i implementar-lo i l'eina ha executat tots els passos sense mostrar-los i, per tant, no s'ha entès tot el procés dut a terme i la complexitat que suposa. Addicionalment, les pàgines a clonar són finites, només aquelles que l'aplicació reconegui i tingui inventariades. Per tant, és un recurs força limitat.

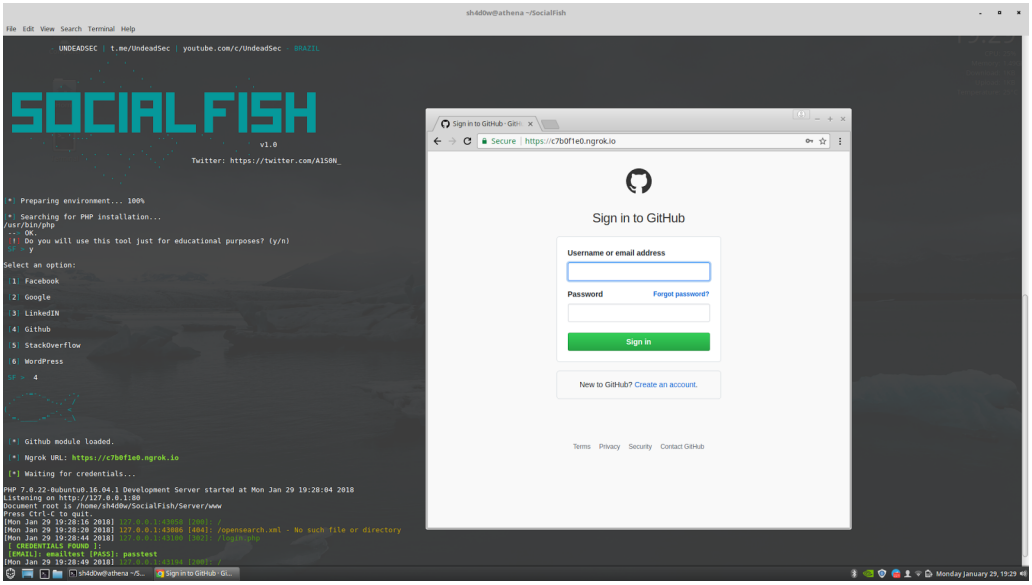


Figura 3: SocialFish.

3. Metodologia i desenvolupament del projecte:

La metodologia que s'ha emprat és la coneguda com CDIO, sigles de l'anglès *Conceive, Design, Implement and Operate* (Concebre, Dissenyar, Implementar i Operar) la qual ha estat adquirida en diversos projectes al llarg del grau d'enginyeria.

La tasca principal que s'ha desenvolupat en aquest projecte és la simulació d'un atac de phishing. Per tal de ser capaç de realitzar aquesta tasca, primerament ha calgut un llarg procés d'investigació i aprenentatge en aquest àmbit. Un cop adquirits els coneixements i procediments necessaris, s'han realitzat el disseny tan del projecte en general com de cadascuna de les eines. Tot seguit s'han posat en pràctica els dissenys de la manera més eficient possible i, finalment, s'han executat amb el fi d'obtenir resultats posteriorment analitzats.

3.1. Recerca

El primer procés que s'ha seguit ha estat de recerca. La idea d'aquest projecte sorgeix de treballar en un departament antiphishing d'una empresa, on s'han obtingut uns primers coneixements sobre què és un phishing, com es pot detectar, de quines parts està format, mètodes per reportar i tancar un cas, com es classifiquen, etc. S'ha adquirit la metodologia emprada pels professionals de la ciberseguretat en la detecció, prevenció i estudi, així com observat l'impacte que causa aquesta amenaça a la societat.

Mentrestant s'ha profunditzat en la matèria per tal de ser capaç d'implementar un atac simulat el qual participi de tot el procés, des de la creació fins al tractament de les dades sostretes de les víctimes. Aquest exercici s'ha realitzat principalment de forma autodidacta portant a terme un llarg procés d'investigació i recull de dades les quals han estat posteriorment destriades, contrastades i estudiades.

A més a més de recursos públics, s'han investigat aquells que són emprats a l'entorn laboral. Cal fer especial incís en què cap eina ni procediment propi de l'empresa ha estat utilitzat ni esmentat en aquest document ni en cap altre dels que formen part d'aquest treball, respectant el compromís de privacitat acordat.

Finalment, els conceptes adquirits han estat recollits en documents per poder ser consultats, no només a l'hora de realitzar aquest treball, si no també en l'educació i conscienciació d'aquesta disciplina.

En aquests documents, recollits als apèndixs, s'estudia d'una banda la història, el funcionament i l'evolució del correu electrònic, el vector més comú en aquest atac i eina utilitzada per gran part de la població. Així doncs, es consideren tots aquests usuaris víctimes potencials de phishing i, per tant, necessiten una educació per evitar-ho. D'altra banda, es fa una introducció a l'Enginyeria Social i s'aporta informació sobre el phishing, des de la definició, detecció i classificació fins a casos més comuns i exemples succeïts a la vida real.

3.2. Disseny

3.2.1. Disseny general de l'atac

Abans de començar a implementar l'atac, cal dissenyar-lo. D'aquesta manera es poden reduir i, fins i tot, evitar retards, imprevistos i resultats erronis.

El primer que cal pensar és a quina empresa o servei suplantar la identitat. Els casos més comuns, tal i com es pot observar a l'apartat "6. Casos més freqüents" de l'apèndix G són plataformes online de pagament o de servei d'altres els quals requereixen el pagament d'una quota i, per tant, un número de compte o de targeta bancària.

S'ha decidit realitzar la pràctica en un entorn simulat, amb màquines virtuals del programa Virtual Box, en comptes de públic per evitar conflictes legals i que el cas sigui detectat i clausurat. Addicionalment, donat que es tracta d'una investigació a l'Escola Superior d'Enginyeria de Telecomunicacions de la Universitat Politècnica de Catalunya, s'ha escollit la pàgina web de l'Atenea, servei de Moodle per intercanviar informació docent entre els alumnes i els professors.

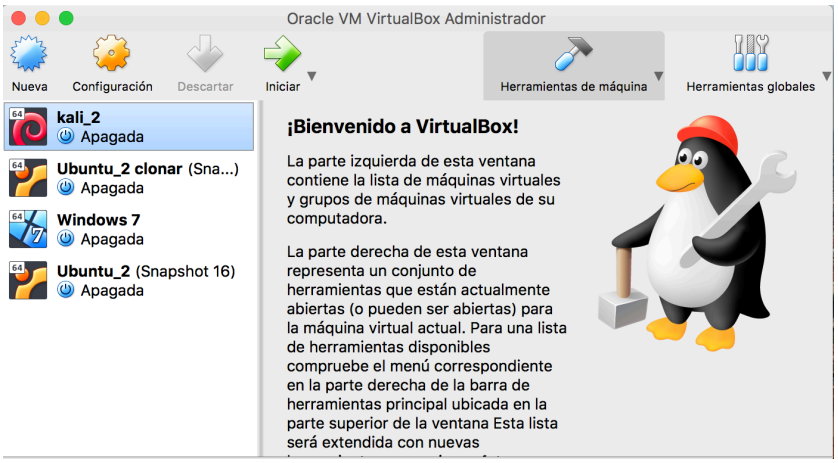


Figura 4: Pàgina d'inici de Virtual Box amb les màquines virtuals utilitzades.

Tal i com s'explica a l'apartat "2.2.1 Definició", un phishing pot propagar-se per diversos vectors: *email* (de l'anglès *electronic mail*), trucada telefònica, SMS o missatgeria instantània. Com que el primer és el més comú i el més estudiat, s'ha decidit utilitzar aquest. També cal tenir en compte que és el més utilitzat i adequat en el servei escollit.

En resum, s'ha decidit simular com a *target* de l'atac els alumnes de la UPC per mitjà de l'Atenea. Acte seguit cal triar les dades que es volen sostreure. S'han escollit les dades d'accés, és a dir, usuari i contrasenya tenint en compte que són compartides per altres pàgines de la universitat on es poden adquirir dades personals com l'adreça, número de telèfon, DNI, compte bancari, etc.

S'ha decidit realitzar 3 simulacions amb l'objectiu de representar els casos més habituals a la realitat:

La primera consta d'un atac bàsic de phishing i, a l'hora, el més comú. Comença amb un correu electrònic on el remitent es fa passar per un professor de l'escola indicant als alumnes que les notes d'un hipotètic control parcial estan disponibles a Atenea. Aquest conté un enllaç per obtenir, suposadament, accés a aquestes puntuacions. No obstant,

l'enllaç redirigeix a una web que simula ser la pàgina principal d'Atenea. Aquí es demana a la víctima les dades d'accés, les quals són robades per l'atacant i guardades per accedir-hi posteriorment. El propòsit d'aquest cas és mostrar el phishing més observat a la realitat.

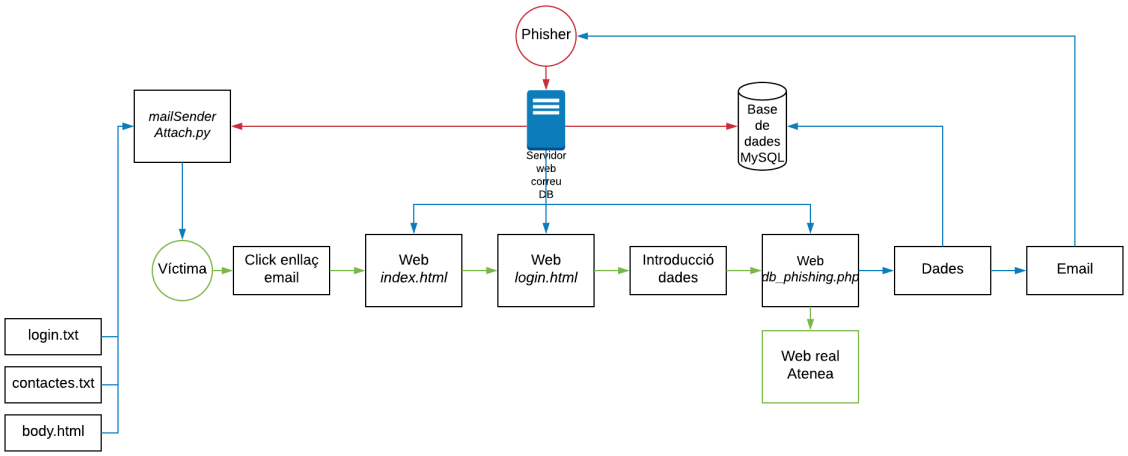


Figura 5: Diagrama de la Simulació 1.

La segona té un format semblant a la primera. Comença també amb un correu electrònic suposadament d'un professor de la UPC. Aquest conté un document adjunt amb les notes d'un hipotètic control parcial en format DNI - nota. També inclou un enllaç que redirigeix, presumptament, a les solucions de l'examen penjades a Atenea. Igual que en el cas anterior, la web és il·lícita amb l'objectiu de sostreure les dades de l'estudiant. El propòsit d'aquest cas és mostrar un phishing on el procediment és innovador, donat l'adjunt, tot i que habitual.

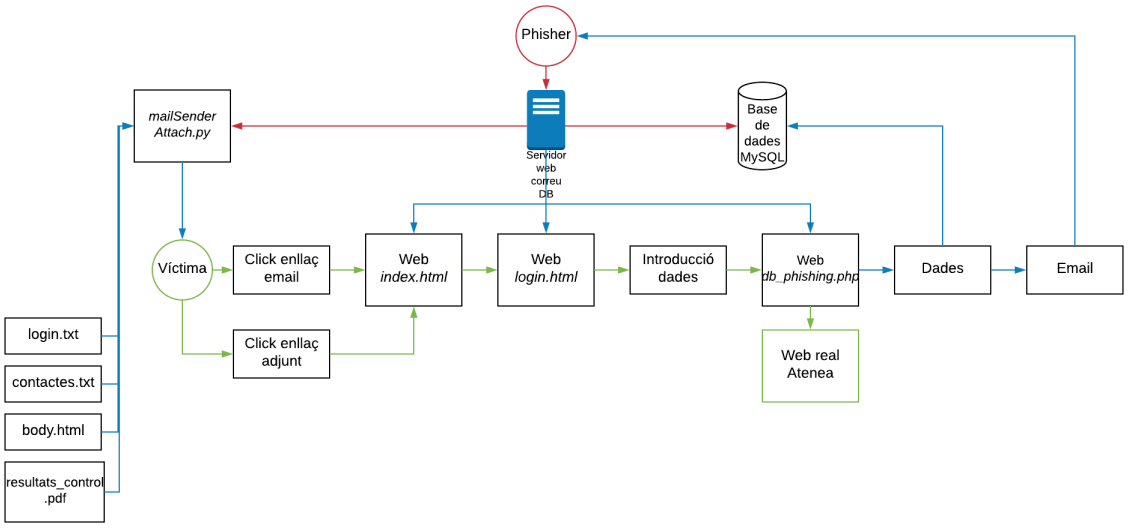


Figura 6: Diagrama de la Simulació 2.

El tercer cas comença amb un correu electrònic d'un fals professor de la universitat el qual facilita als alumnes un software per utilitzar a les pràctiques d'una assignatura.

Quan aquest és executat per la víctima, obre una connexió amb un *host* del *phisher* a través d'una *shell* remota. D'aquesta manera el ciberdelinqüent obté accés a la línia de comanes de l'equip de la víctima, on serà capaç de sostreure informació personal, dur a terme altres atacs, propagar-se per la xarxa, etc.

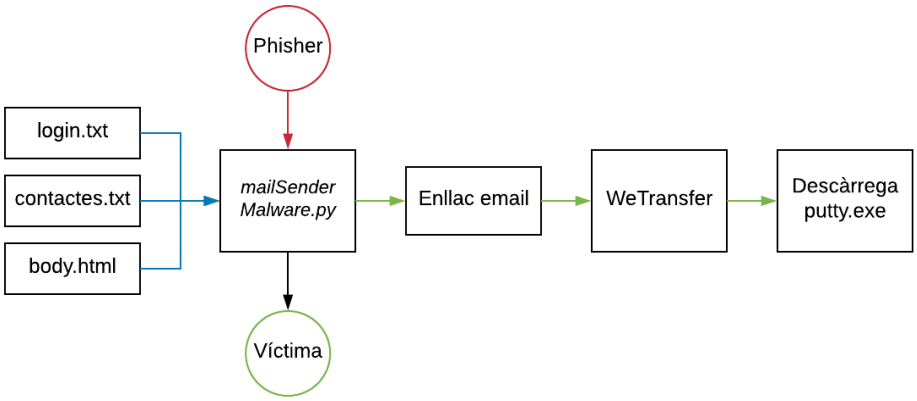


Figura 7: Diagrama de la Simulació 3.

3.2.2. Disseny del correu electrònic

Després del plantejament general, cal dissenyar com implementar cadascun dels passos que el conformen.

El phishing comença amb l'enviament del correu. Donat que els destinataris seran múltiples, sorgeix la necessitat d'automatitzar el màxim possible aquest procediment. La millor manera és creant un *script* que s'encarregui d'enviar el correu. Per escriure aquest fitxer s'ha escollit el llenguatge Python 3 ja que disposa de biblioteques simples i eficients per connectar-se i interactuar amb el servidor SMTP de correu. La seva simplicitat facilita llegir i incloure continguts externs al propi fitxer, la qual cosa permetrà adjuntar documents al missatge, llegir contrasenyes en comptes d'escriure-les de manera visible al propi *script* i donar valor a variables sense incrementar el nombre de línies de codi, com pot ser el cas dels destinataris del missatge.

De bon inici es va plantejar la idea de crear un servidor de correu propi en una màquina virtual amb sistema operatiu Linux. La instal·lació i implementació local era viable però la connexió amb el client de correu o webmail, la implementació dels registres DNS i la publicació a la xarxa suposava un increment de temps i recursos. La segona opció que es va plantejar va ser utilitzar un servei de correu electrònic ja existent i gratuït. L'avantatge addicional és que el domini és conegut a internet, de manera que les comprovacions d'autenticació de domini realitzades pels servidors intermedis i destinataris explicades a l'apartat "3.2 Estàndards de validació" de l'apèndix F no aturaran el missatge. Finalment es va escollir Gmail de Google per la seva fiabilitat, eficiència i simplicitat.

De la comunicació entre el *script* i el servidor de correu electrònic sorgeix la necessitat de conèixer el protocol SMTP: de quines capçaleres disposa, el format d'aquestes, els protocols d'autenticació i comprovació d'autenticitat, els filtres antispam i antiphishing a vulnerar, etc. Tota aquesta informació ha estat recollida a l'apèndix F i utilitzada posteriorment en la implementació dels *scripts*.

El missatge a enviar ha de contenir un enllaç que redirigeixi a la pàgina web fraudulenta. Així doncs, el format d'aquest no pot ser text pla si no HTML. Python posseeix una biblioteca per escollir l'estàndard MIME [26] que es vol aplicar al correu. Addicionalment es pot crear un fitxer HTML [27] que contingui el cos del missatge i ser llegit pel fitxer Python, el qual posteriorment l'ajunti a la resta de capçaleres.

Tal i com s'explica a l'apartat "2.2.2 Spear Phishing" el *Spear Phishing* admet l'enviament de fitxers maliciosos adjunts. Per això s'ha decidit fer una simulació que reflecteixi aquest cas d'ús més innovador, cada vegada més habitual i que pot causar un gran impacte a les víctimes. Fa referència a la tercera simulació explicada a l'apartat "3.2.1 Disseny general de l'atac".

3.2.3. Disseny de la pàgina web

El segon pas del phishing, un cop la víctima ha rebut el correu i ha estat convençuda per accedir a l'enllaç, és dissenyar la pàgina web a la qual aquest redirigeix. Ha de ser el més semblant possible a la pàgina real perquè aquesta cregui que està al *site* autèntic. Addicionalment, a gran part dels casos de phishing s'assigna un domini molt semblant al lícit amb la intenció de confondre la víctima.

Una pràctica habitual és clonar el web real. Hi ha diversos mètodes, però el més senzill i igualment efectiu és consultar el codi font de la vista obtinguda del *site* utilitzant les eines de desenvolupador del navegador web.

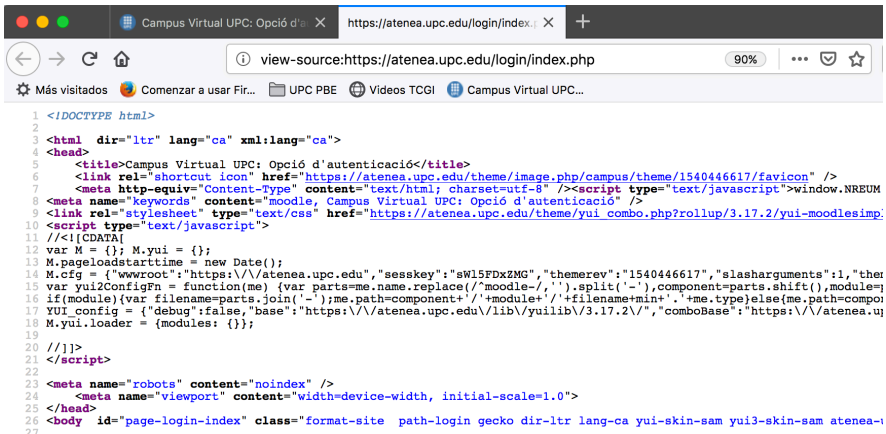


Figura 8: Vista del codi font de la pàgina inicial d'Atenea des del navegador web.

S'estudia l'enviament de les dades personals d'inici de sessió que realitza la pàgina autèntica. L'acció realitzada és un POST [28] a una altra pàgina on es comprova si pertanyen a un usuari existent. Per tant, un cop copiat el codi font cal modificar aquesta acció. El POST s'ha de fer a una altra pàgina en la qual es puguin tractar aquestes dades.

A l'hora d'escollir el llenguatge per a la pàgina web, s'ha tingut en compte que l'original està escrita en HTML i, a més a més, personalment hi estic més familiaritzat. Per al tractament de les dades cal usar un altre llenguatge. Com que forma part del *back-end* [29], s'ha escollit el llenguatge PHP per la seva compatibilitat amb HTML i la seva simplicitat.

El servidor web emprat és Apache2 [30], donada la simplicitat, l'eficiència i les característiques del projecte, a més de tenir un coneixement previ del grau d'enginyeria.

Estudiant diferents casos de phishing, s'ha conclòs que el pas final en gran part de les campanyes consta de realitzar una redirecció a la pàgina real. D'aquesta manera es vol fer creure a la víctima que hi ha hagut un error a l'hora d'introduir les dades en el passos anteriors o que simplement ha finalitzat el procés que se li requeria. Per aquest motiu s'inclou aquesta pràctica a la simulació. S'explica amb més detall a "2.2.4 Detecció de phishing".

A l'atac, les dades que es recullen són l'usuari i contrasenya. Tot i això, a la petició lícita s'envien altres variables per mitjà del mètode POST. Una d'elles és seqüencial i compte els intents d'inici de sessió d'un mateix usuari, ja siguin correctes o erronis, seguint un format específic. L'altra té un format més complex ja que comença amb les lletres "LT" seguit de la data en format Unix i una seqüència aleatòria codificada. Aquest estudi s'ha fet amb el propòsit d'iniciar sessió just després de la redirecció, de tal manera que semblés encara més realista i l'usuari no pogués sospitar que es tracta d'un cas de phishing. Donat que no ha estat possible aquesta descodificar última seqüència, no s'ha realitzat aquesta acció. Aquesta és una mesura habitual en els inicis de sessió de moltes pàgines web, justament per evitar aquests tipus de pràctiques.

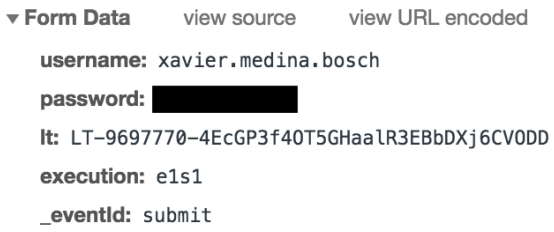


Figura 9: Dades transmeses per la petició POST a la web d'Atenea.

3.2.4. Disseny del tractament de dades

Ja s'ha dissenyat el punt d'interacció amb l'usuari, on introduirà les seves credencials d'accés. Tot seguit cal dissenyar com tractar aquestes dades.

Estudiant el comportament dels cibercriminals, s'ha observat que les dues pràctiques que més duen a terme són: guardar-les en una base de dades i enviar-les per *email*. La primera permet crear un registre amb tota la informació extreta. La segona notifica el criminal que té disponible nova informació en el mínim temps el qual fa possible, a més a més de no haver de comprovar periòdicament si hi ha una nova entrada a la base de dades, fer-ne ús abans de que la víctima se n'assabenti i les pugui modificar.

Com que no són excloents l'una de l'altra, s'ha decidit dur a terme ambdues en aquest treball per evidenciar els casos més freqüents de la realitat.

La majoria del procés s'executa des d'una mateixa màquina virtual Linux que actua com a servidor de correu electrònic i web fent servir Apache2 i PHP. Així doncs, s'ha decidit utilitzar MySQL [31] per emmagatzemar les dades i d'aquesta manera treballar en un entorn LAMP [32].

3.3. Implementació

El procés d'implementació s'ha dut a terme seguint el disseny de l'apartat "3.2 Disseny" i aplicant els coneixements obtinguts de la recerca esmentada a l'apartat "3.1 Recerca". Per tant, en aquest apartat se seguirà la mateixa classificació que en l'anterior.

3.3.1. Implementació del correu electrònic

Per enviar el correu electrònic s'ha creat un *script* en Python per a cadascuna de les 3 simulacions. Seguidament s'expliquen les funcionalitats generals i comunes i, a l'apèndix E es detallaran les particularitats de cadascun d'ells juntament amb el codi a l'apèndix G.

Els *scripts* s'han implementat seguint un mateix ordre, essent modificats en segons les particularitats de cada simulació.

- **Importació**: S'importen les biblioteques i mòduls de Python necessaris per a la interacció amb el servidor SMTP.
- **Autenticació**: Es realitza la connexió amb el servidor SMTP de Gmail. Tot seguit s'inicia sessió amb les dades de correu electrònic. Aquestes han estat escrites en un fitxer a part i llegides pel *script*. D'aquesta manera es manté la privacitat de la contrasenya i es pot canviar fàcilment de compte sense haver de modificar el codi.
- **Destinataris**: Es llegeixen les adreces d'un fitxer de text extern, ja que aquests hauran estat obtinguts prèviament a l'atac i emmagatzemats.
- **Missatge**: S'afegeixen les variables del missatge. El cos del missatge conté un enllaç, per tant no pot ser escrit en text pla. És escrit en un fitxer HTML, llegit posteriorment pel *script* i concatenat a la resta de contingut del missatge. Igual que en el cas anteriors, permet modificar el cos del missatge enviat fàcilment sense modificar el codi. S'indiquen els valors de les capçaleres i finalment s'adhereixen totes les dades.
- **Enviament**: Per últim s'envien el *email* i es finalitza la connexió amb el servidor.

La segona simulació té un apartat addicional per incloure el fitxer adjunt al correu. La tercera simulació, com que té un format gairebé igual que la primera, segueix els mateixos passos.

3.3.2. Implementació de la pàgina web

Per poder fer accessible una pàgina web des del navegador d'altres *hosts*, cal implementar un servidor web. Com s'ha indicat a l'apartat "3.2.3 Disseny de la pàgina web" s'ha implementat Apache2. El passos seguits i la configuració es troben a l'apartat "4. Instal·lació del servidor web" de l'apèndix E.

Per accedir al servidor web i, per tant, a la pàgina creada, cal indicar la IP d'aquesta màquina. Per tant, cal configurar una IP estàtica tal i com es mostra a l'apartat 5 de l'apèndix E. Com que l'entorn de l'atac dut a terme en aquest projecte és virtual, és a dir privat, la IP emprada pel phisher serà la privada. En un cas real es necessitaria conèixer la IP pública visible des d'internet i configurar regles NAT per tal de redirigir el tràfic a la IP privada del servidor web, així com encaminar i empaquetar correctament el tràfic sortint. Per fer més accessible i creïble aquesta web, caldria assignar un domini que resolgués a la IP pública i també crear registres DNS que es publiquessin a internet. En aquest projecte, s'ha modificat el registre "hosts" de la màquina virtual que simula la víctima indicant un domini a la IP privada del servidor, donat que estan dins la mateixa xarxa. Aquest domini serà semblant al lícit.

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
        192.168.1.68    atenea.upc-edu.com
q
```

Figura 10: Fitxer hosts de la màquina virtual que simula la víctima.

L'accés a la web d'Atenea consta de dues pàgines: la primera permet iniciar sessió, indicar si hi ha problemes d'accés o escollir l'idioma i la segona, l'accés al compte personal on es demanen les credencials. Per fer més creïble l'atac, s'han replicat ambdues pàgines.

Per a la primera pàgina, s'ha copiat el codi font en un fitxer HTML on s'ha modificat la redirecció de l'opció "Iniciar sessió" perquè enllaci amb la segona pàgina.

Per a la segona pàgina també s'ha copiat el codi font en un fitxer HTML. En aquest cas s'ha modificat el formulari per tal que el POST que conté les dades introduïdes es dirigeixi a una tercera pàgina, la qual no serà visible per l'usuari, on seran tractades. S'explica a l'apartat següent "3.3.3 Implementació del tractament de dades".

Per tal que la vista sigui la mateixa s'han replicat els directoris i s'han emmagatzemat les mateixes imatges i fitxers CSS a la ruta publicada per l'Apache.

3.3.3. Implementació del tractament de dades

La tercera pàgina s'ha creat en un fitxer PHP. Aquesta recull les dades que conté el POST, les emmagatzema a la base de dades MySQL i les envia per *email*, tal i com s'explica a "3.2.4 Disseny del tractament de dades". Finalment redirigeix a la pàgina real d'accés d'Atenea per seguir el procediment explicat a l'apartat "3.2.3 Disseny de la pàgina web".

La base de dades ha estat implementada localment al propi servidor. Per accedir-hi es fa des del propi terminal de la màquina, sense fer servir agents web de tercers. S'ha creat la base de dades **db_tfg** la qual conté la taula **phishing_atenea**. La implementació es detalla a l'apartat 3 de l'apèndix E.

Aquestes dades també són enviades per correu electrònic, tal i com s'ha explicat a l'apartat "3.2.4 Disseny del tractament de dades". En el mateix arxiu PHP on es recullen les dades inserides, es fa ús de l'extensió "mail" [33] d'aquest llenguatge per enviar-les per *email*. Donat que la informació no s'ha de fer pública i té un objectiu informador per a l'executor, s'aprofita el compte de correu i s'utilitza com a remitent i destinatari d'aquest missatge. El codi es detalla a l'apartat 1 de l'apèndix E.

3.3.4. Implementació del Malware

Per a la creació del fitxer maliciós de la tercera simulació s'ha recorregut al sistema operatiu Kali Linux implementat en una altra màquina virtual. Aquesta eina és utilitzada per a auditories de ciberseguretat, defensa de sistemes i, en altres casos, per a atacs també. Conté vora de 600 programes preinstal·lats, entre els quals es troba Metasploit.

Metasploit és un programari lliure que proporciona informació sobre vulnerabilitats de seguretat i s'utilitza per a la realització de tests de penetració o *pentesting*. Un dels seus mòduls, anomenat "msfvenom" [34], s'encarrega de la generació i codificació de *payloads*. Amb l'execució d'aquest, s'ha generat un fitxer executable que simula ser el Putty.exe, programa utilitzat per realitzar connexions remotes entre hosts. Realment s'ha

implementat l'obertura d'una connexió des de l'equip on s'executi fins a l'adreça IP de la màquina Kali per un port indicat. L'atacant, que escoltarà per aquest port concret, rebrà una *shell* remota de l'equip de la víctima la qual donarà accés al sistema.

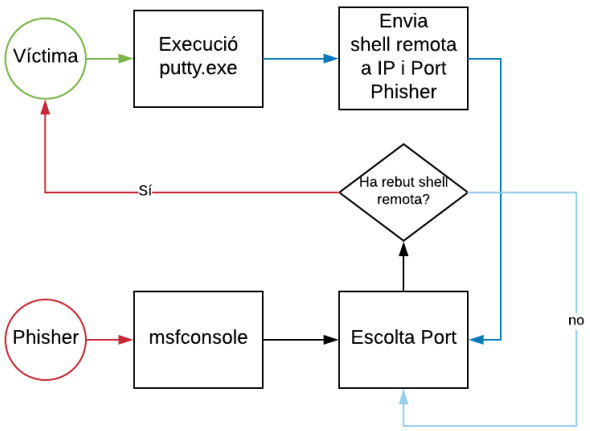


Figura 11: Diagrama d'execució del malware.

A l'apartat 2.3.1 de l'apèndix E s'explica amb detall els passos seguits per a la implementació d'aquest fitxer.

3.4. Execució

A continuació es mostra l'execució de les tres simulacions de phishing explicades en els punts anteriors. Cadascuna s'explicarà per separat des de l'inici fins al final per observar detalladament cada cas.

3.4.1. Simulació 1

En primer lloc s'executa el *script* encarregat de l'enviament dels *emails* anomenat **mailSender.py**. Es parteix del supòsit que s'ha obtingut una llista d'adreces de correus electrònics per un dels mitjans de l'apartat "2.2.6 Obtenció de contactes", la qual és llegida per aquest. Un cop enviat, cal esperar que la víctima l'obri i hi caigui.

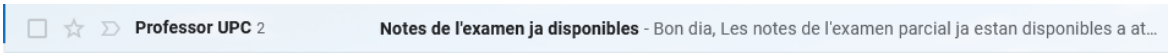


Figura 12: Vista prèvia del correu rebut per la víctima

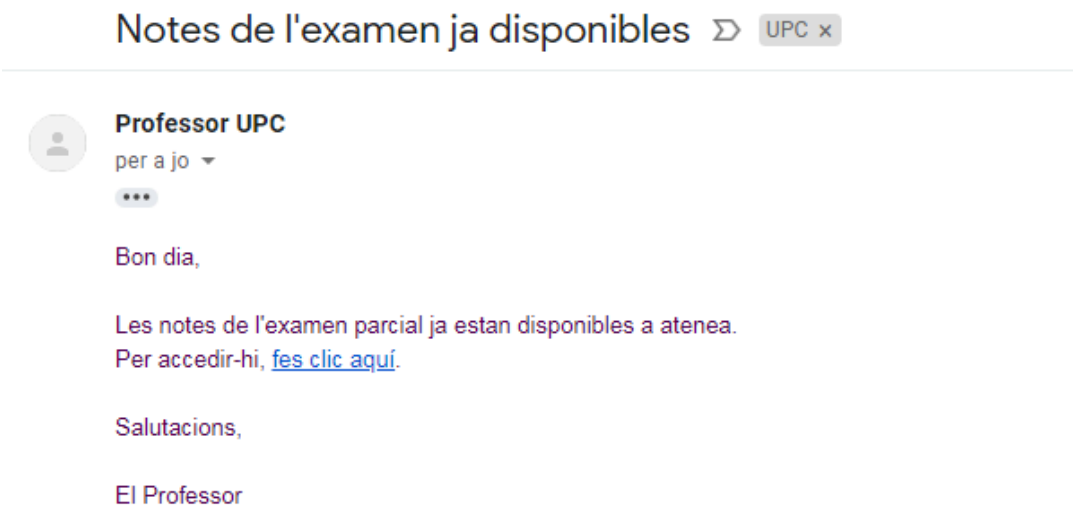


Figura 13: Correu electrònic rebut per la víctima.

Un cop es fa clic a l'enllaç, s'obre a l'explorador la primera de les webs del phishing: la suposada pàgina inicial d'Atenea, anomenada **index.html**. Es pot observar a la imatge com la URL no és l'original, però sí semblant.

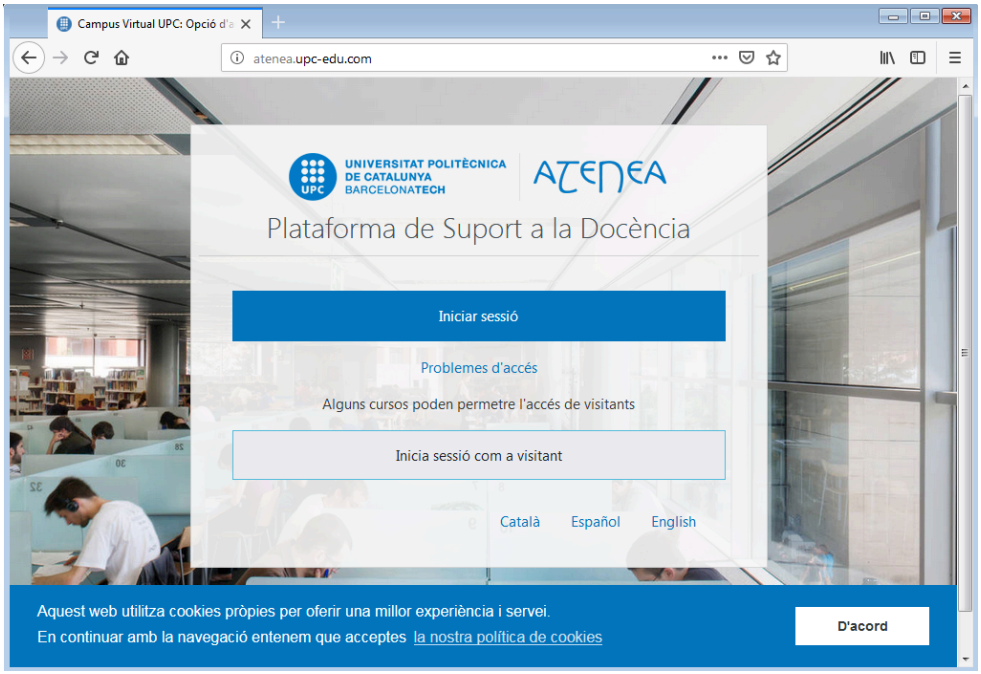


Figura 14: Pàgina d'inici fraudulenta.

Quan l'usuari premi "Iniciar sessió" es redirigirà a la pàgina de *login* clonada, anomenada **login.html**:

Figura 15: Pàgina d'accés fraudulenta.

Després d'introduir les dades i prémer "Entra", aquestes es transmeten a la pàgina de tractament de dades, anomenada **db_phishing.php**, on s'envien per correu al phisher, s'emmagatzemen a la base de dades MySQL i redirigeix l'usuari a la pàgina real d'Atenea.

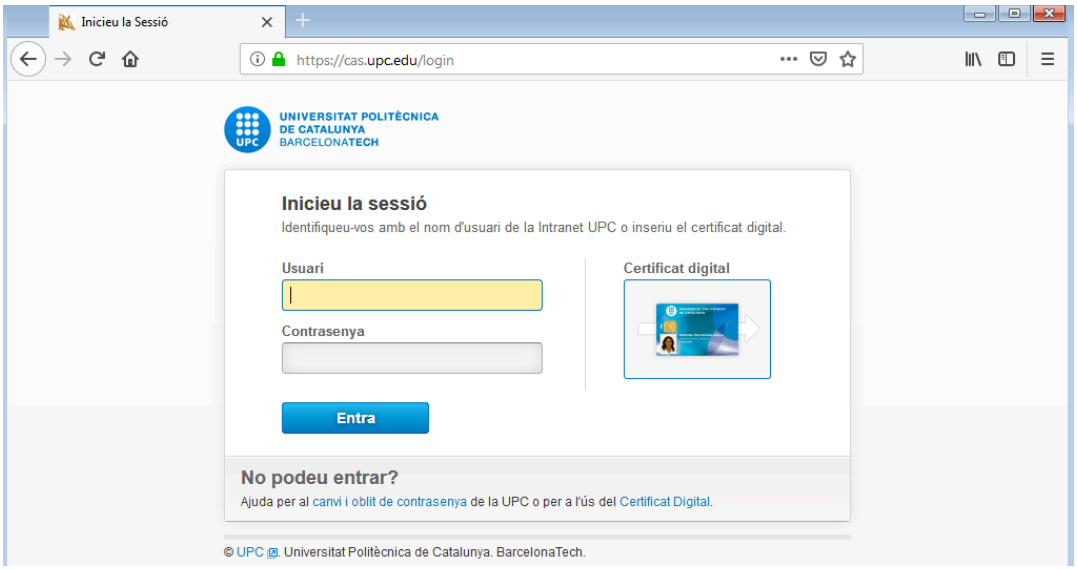


Figura 16: Pàgina real d'accés a Atenea.

```
mysql> mysql> select * from phishing_atenea;
+---------------------+---------------------+-----------------+
| Data                | Usuari              | Contrasenya     |
+---------------------+---------------------+-----------------+
| 2019-01-10 03:12:37 | xavier.medina.bosch | contrasenya1234 |
| 2019-01-14 09:50:40 | xavier.medina.bosch | contrasenya1234 |
+---------------------+---------------------+-----------------+
```

Figura 17: Taula de la base de dades MySQL amb les dades introduïdes al phishing.

Figura 18: Correu que rep el phisher amb les dades sostretes.

3.4.2. Simulació 2

El procés que segueix l'atac en aquesta simulació és el mateix que en l'anterior però canvien els fitxers executats i els resultats.

Primerament s'executa el fitxer **mailSenderAttachment.py** el qual, anàlogament al *script* de l'apartat anterior, envia el *email* a les víctimes.

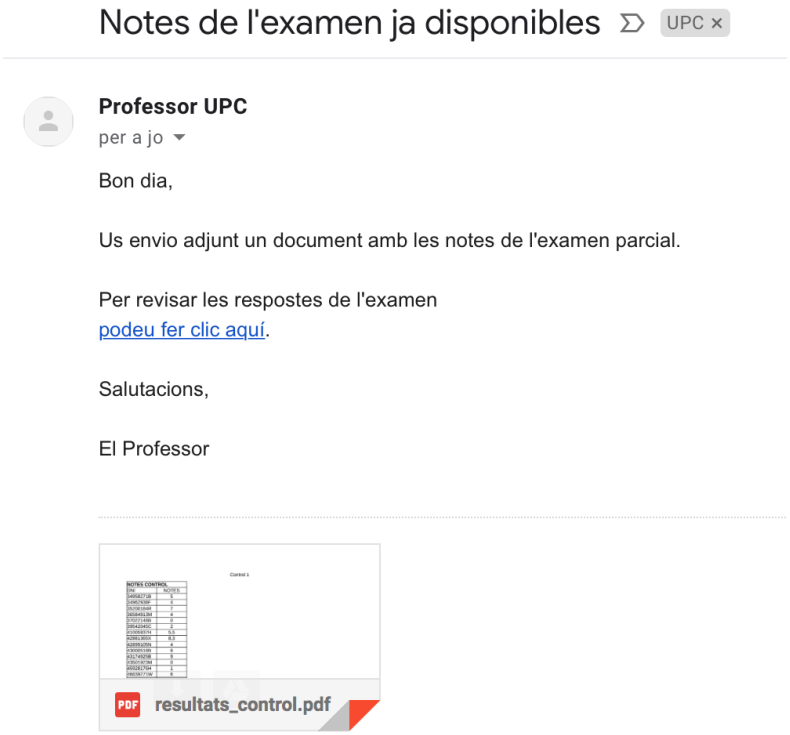
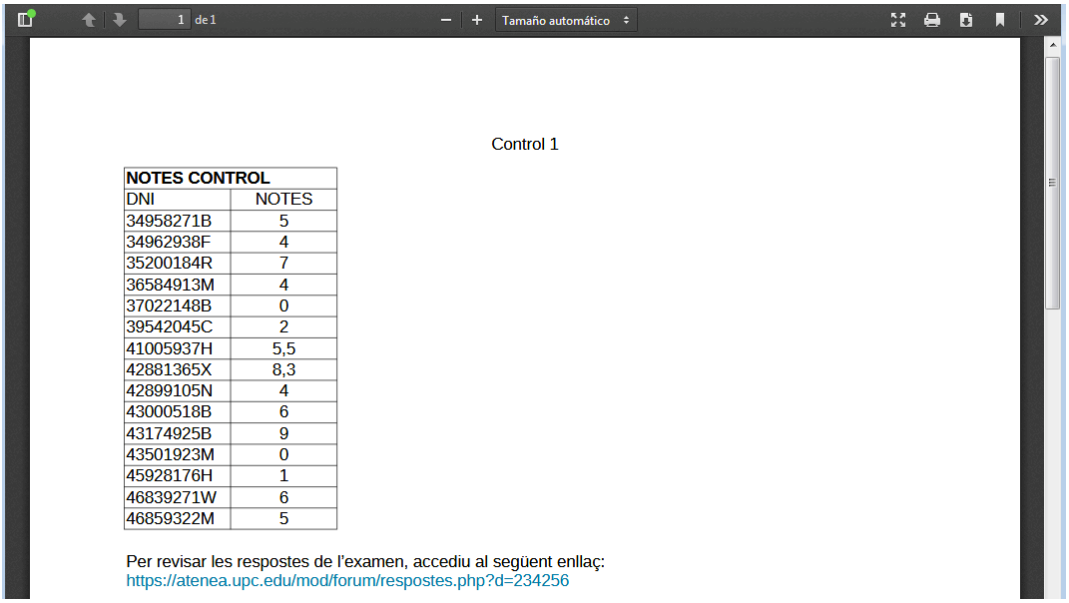


Figura 19: Correu electrònic rebut per la víctima.



Control 1

NOTES CONTROL	
DNI	NOTES
34958271B	5
34962938F	4
35200184R	7
36584913M	4
37022148B	0
39542045C	2
41005937H	5,5
42881365X	8,3
42899105N	4
43000518B	6
43174925B	9
43501923M	0
45928176H	1
46839271W	6
46859322M	5

Per revisar les respostes de l'examen, accediu al següent enllaç:
https://atenea.upc.edu/mod/forum/respostes.php?d=234256

Figura 20: Document adjunt al correu amb l'enllaç fraudulent.

En aquest punt la víctima accediria, mitjançant l'enllaç del PDF o el del cos del missatge, a la web d'Atenea falsificada tal i com es mostra a la figura 20. A partir d'aquí, el procés segueix de la mateixa manera que en el cas anterior.

3.4.3. Simulació 3

El primer pas és enviar els *emails* a les víctimes, procés que executarà el *script* **mailSenderMalware.py**. El correu electrònic es veurà de la manera següent:

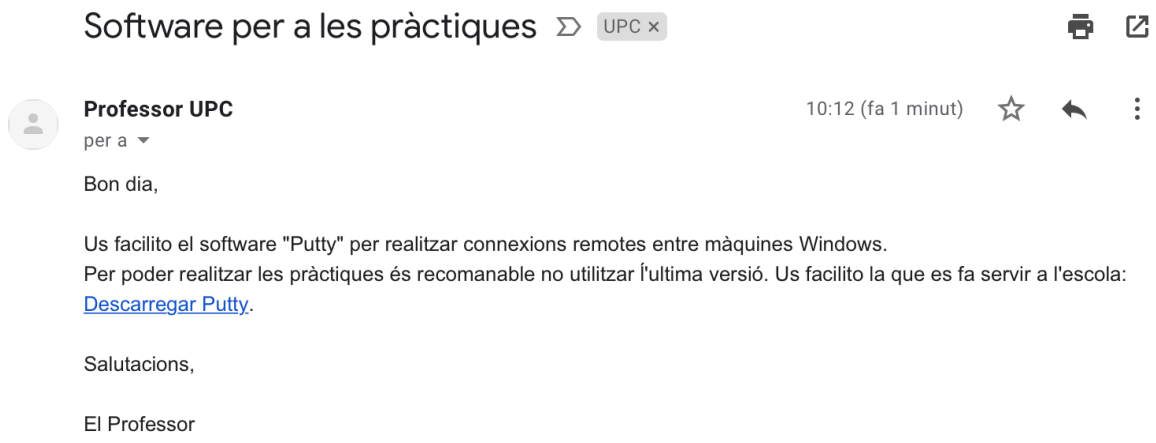


Figura 21: Correu electrònic rebut per la víctima.

Quan la víctima premi sobre "Descarregar Putty" s'obre al navegador una pàgina de WeTransfer des de la qual es pot descarregar el fitxer.

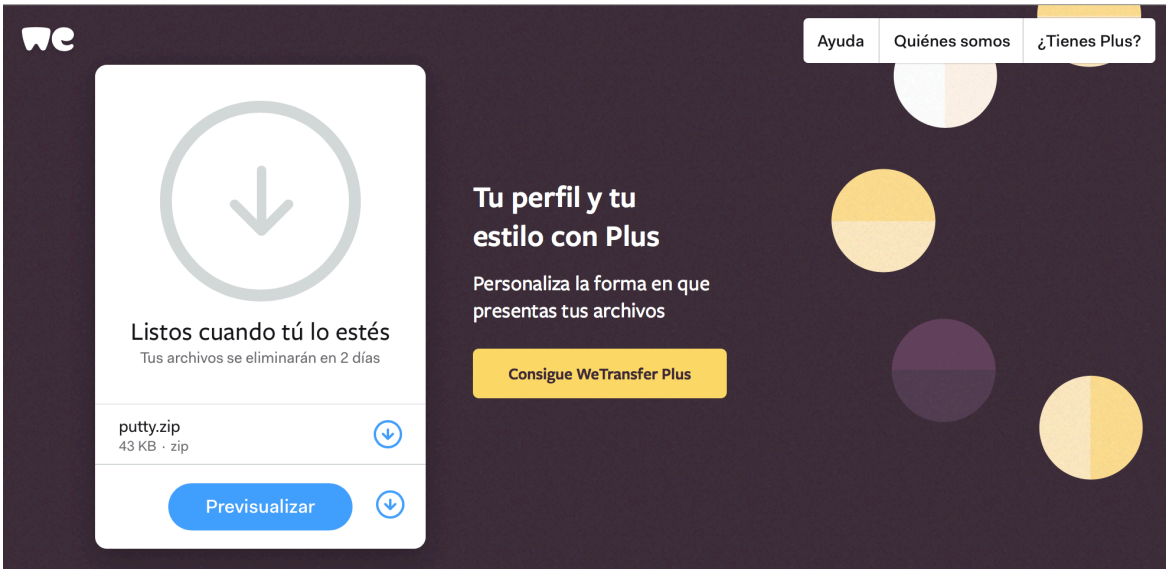


Figura 22: Pàgina de descàrrega del fitxer maliciós.

Un cop descarregat, serà executat per la víctima.

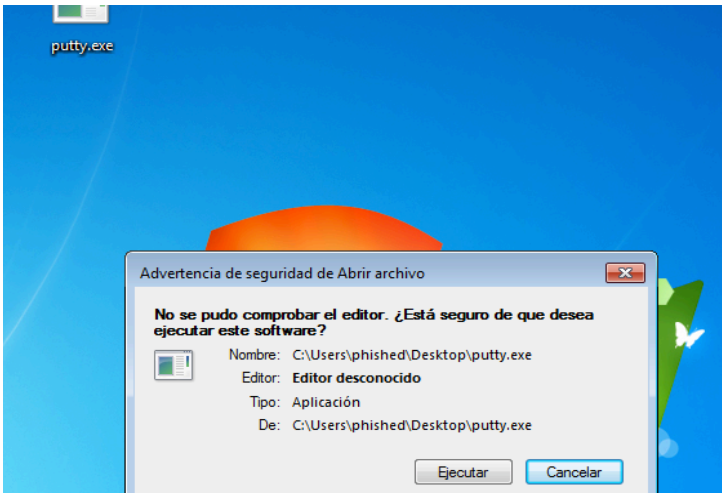


Figura 23: Escriptori de la víctima iniciant l'execució del malware.

Paral·lelament, l'atacant iniciarà el procés que escolta les connexions entrants a la seva IP pel port indicat. Quan la víctima executi el *software*, observarà la sessió activa establerta amb la connexió.

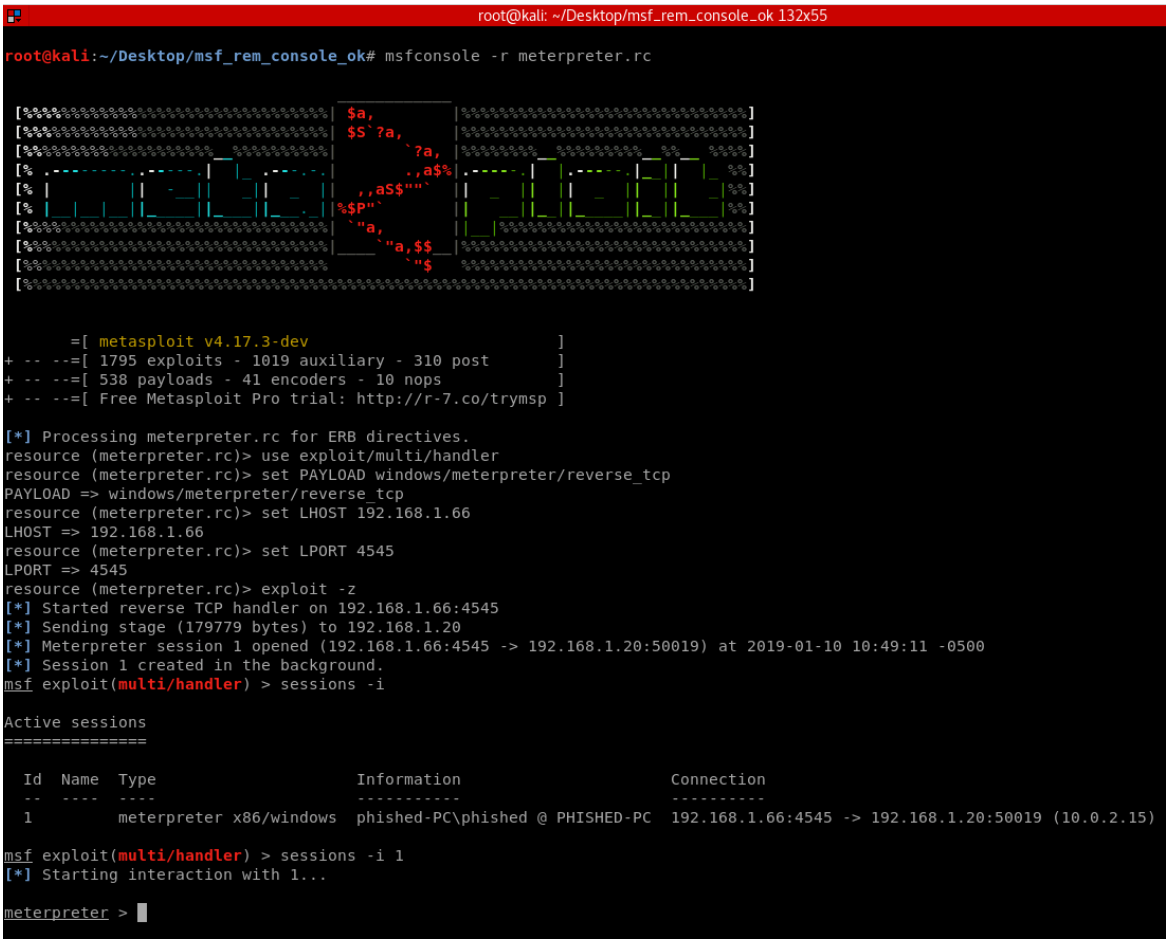


Figura 24: Connexió establerta entre l'equip de la víctima i el de l'atacant.

El ciberdelinqüent ja té accés remot a la màquina de l'alumne per mitjà del procés creat de l'execució del *malware*. Si aquest tanca aquest procés també tanca la connexió. Així, si sospita d'una execució maliciosa es perdrà l'accés. És per això que el primer que ha de fer el phisher és migrar el procés.

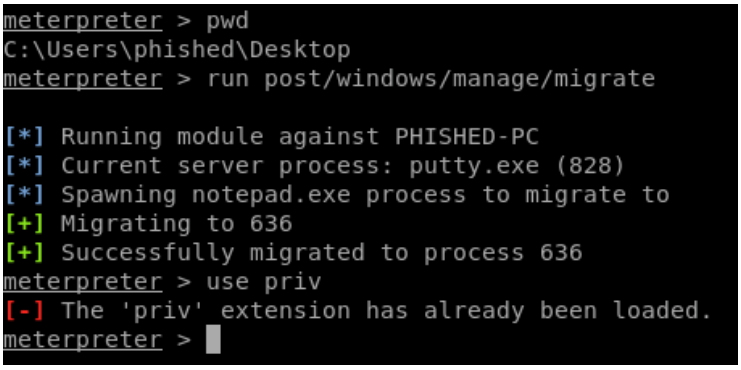


Figura 25: Accés rutes del host víctima, migració de procés i obtenció de privilegis.

Ara la connexió ja és estable sense dependre del procés del *software* maliciós. A partir d'aquí, es pot obtenir accés a tots els directoris de la màquina de la víctima i realitzar qualsevol atac i fuga de dades.

L'exemple dut a terme ha estat l'execució d'un *keylogger* [35], el qual enregistra totes les tecles premudes pel teclat. D'aquesta manera, quan accedeixi a Atenea quedaran gravades les dades d'accés. L'avantatge és que no només s'obtenen les dades de les simulacions anteriors, si no molts més. Addicionalment, si la víctima es dóna compte de l'atac, encara que elimini l'arxiu i executi l'antivirus, la connexió seguirà establerta.

```
meterpreter > ls -ltr
Listing: C:\Users\phished\Desktop
=================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  1061   fil   2019-01-10 10:16:14 -0500  Firefox.lnk
100666/rw-rw-rw-  436    fil   2019-01-10 08:38:42 -0500  desktop.ini
100777/rwxrwxrwx  73802  fil   2019-01-01 06:24:48 -0500  putty.exe
100666/rw-rw-rw-  1304   fil   2009-07-14 00:54:32 -0400  Notepad.lnk
```

Figura 26: Accés als fitxers del host de l'atacat.

```
meterpreter > run post/windows/capture/keylog_recorder

[*] Executing module against PHISHED-PC
[*] Starting the keylog recorder...
[*] Keystrokes being saved in to /root/.msf4/loot/20190110105449_default_10.0.2.15_host.windows.key_546419.txt
[*] Recording keystrokes...
```

Figura 27: Execució del keylogger.

```
root@kali: ~ 142x27
root@kali:~# vim /root/.msf4/loot/20190110105650_default_10.0.2.15_host.windows.key_056128.txt
```

Figura 28: Obertura del registre creat pel keylogger.

A continuació es pot observar com s'ha accedit a la pàgina d'Atenea i s'han introduït les dades d'accés.

```
root@kali: ~ 144x27
Keystroke log from notepad.exe on PHISHED-PC with user phished-PC\phished started at 2019-01-10 10:56:50 -0500

<^H>u
<^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H>atenea
.upc.edu<CR>^M

xavier.med
ina.bosch<Tab>contrasenya12
3<CR>^M
```

Figura 29: Registre creat pel keylogger.

3.5. Enquesta

Tan dins la feina, treballant amb casos de phishing reportats, com fora he percebut que existeix cert grau de desconeixement respecte d'aquest tipus d'atac. Així doncs la hipòtesi inicial és que existeix desconeixement entre la gent, ja sigui parcialment o totalment, envers un atac de phishing, com es pot detectar i evitar i quines repercussions pot causar.

S'ha creat una enquesta amb preguntes relacionades amb el phishing i amb la interacció entre l'usuari i aquests casos. Es pretén validar o refutar la hipòtesi plantejada i avaluar si s'actua de manera correcta. Addicionalment, s'ha creat un document explicatiu en el qual es parla sobre la detecció i la prevenció del phishing, així com de les variants que existeixen i es mostra algun exemple pràctic. S'ha afegit al final de l'enquesta i està dirigit a tots els públics, ja siguin persones tècniques o no, de qualsevol edat, etc.

A l'apèndix H es troba l'enquesta i el document, anomenat "**Decàleg de bones pràctiques**".

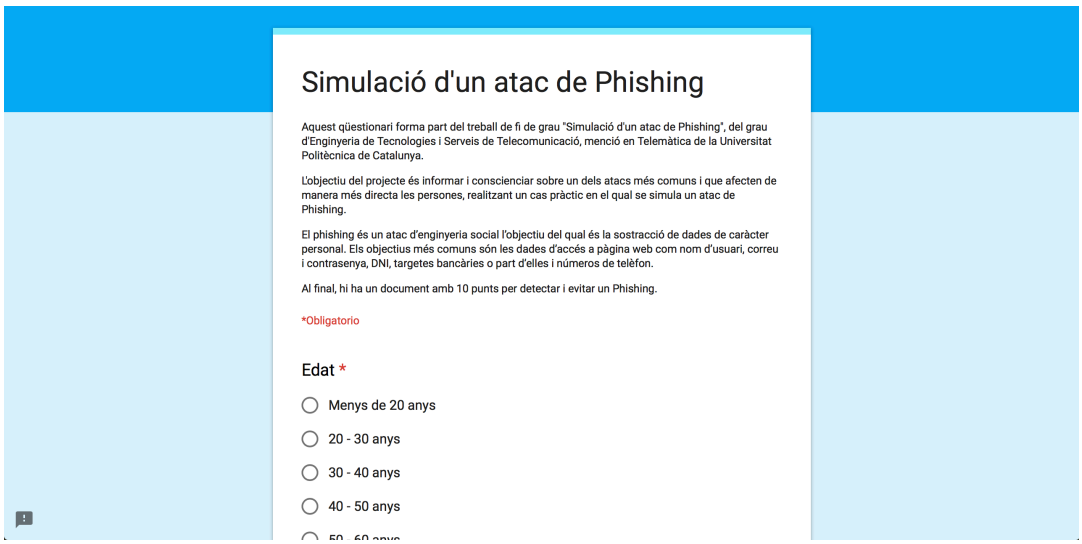


Figura 30: Vista de l'enquesta des del navegador.

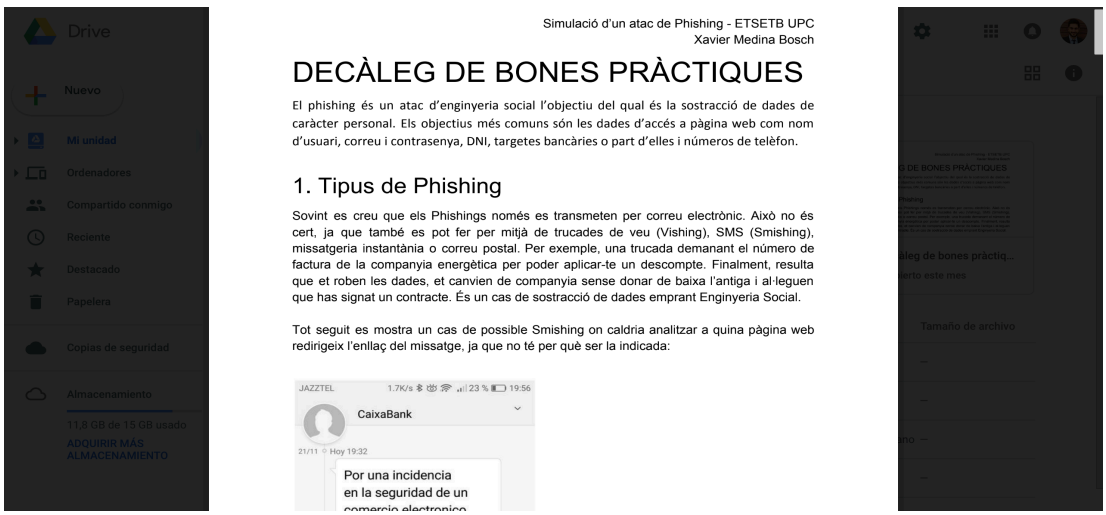


Figura 31: Vista del Decàleg de bones pràctiques des del navegador.

4. Resultats

4.1. Simulacions

L'objectiu d'un phishing és obtenir dades personals d'altres persones i en totes tres simulacions ha estat possible:

En les dues primeres, les dades introduïdes per les víctimes acaben en mans de l'atacant per mitjà dels dos mètodes més comuns a la realitat. Així, tant per correu electrònic com en una base de dades, el phisher acaba obtenint satisfactòriament la informació sol·licitada a l'atac.

En la tercera, la connexió entre l'equip de la víctima i el del phisher és satisfactòria. Tenint en compte l'exemple del *keylogger,* la informació és transmesa i emmagatzemada correctament al host del ciberdelinqüent. Addicionalment, donat l'èxit d'aquesta comunicació, el ventall de possibilitats és molt més extens. Per tant es considera que aquest atac també ha estat realitzat amb èxit.

L'objectiu d'aquestes simulacions de phishing és mostrar el procés que segueix aquest atac per poder entendre tots i cadascun d'aquests passos. Aquesta informació ha de servir per tenir més coneixement de l'amenaça amb el propòsit d'augmentar la probabilitat de prevenir aquests tipus d'atacs.

4.2. Enquesta

La participació de l'enquesta ha estat de 141 persones. D'aquestes, un 56% afirmen haver rebut algun un phishing. És possible que aquelles que han contestat que no n'hagin rebut algun però no en siguin conscients. De les 79 respostes afirmatives tan sols 6 n'han estat víctimes, el qual representa un 7,6%. Els resultats de cada pregunta i les conclusions específiques que se n'extreuen es troben a l'apartat "2. Resultats" de l'apèndix H.

5. Pressupost

Tot el software utilitzat en aquest projecte és programari lliure, de manera que no es tindrà en compte cap cost en aquest concepte.

Per calcular el salari d'un enginyer junior, es té en compte els requisits de pràctiques empresarials marcats per la universitat, els quals determinen un mínim de 8€ l'hora.

El temps dedicat al treball ha estat de 40 hores setmanals i la durada del projecte, de 16 setmanes.

Així doncs, s'obté:

$$\frac{8€}{hora} \times \frac{40\ hores}{setmana} \times 16\ setmanes = \mathbf{5120}€$$

6. Conclusions i desenvolupament futur

6.1. Conclusions

Aquest projecte m'ha permès endinsar-me a la ciberseguretat, un sector molt extens que forma part de la vida de la gran majoria de les persones ja sigui de manera conscient o no. Concretament m'ha permès conèixer detalladament els atacs de phishing, profunditzant no tan sols en la detecció d'aquests, si no també en tots els processos de creació i de defensa. Per tant m'he posat en la pell d'un atacant, conegut com a "red team" i en la de defensa, "blue team".

No només a nivell tècnic, si no personal, m'ha aportat molta experiència quant a la realització d'un projecte complet i individual. La recerca de conceptes i procediments, la gestió del temps, l'aprenentatge i el contacte amb persones que porten anys dedicades a aquest sector m'ha aportat un enfocament diferent a l'hora de treballar, gestionar el temps i els recursos, conèixer la ciberseguretat des de dins i decidir si seguir en aquesta vessant de la telemàtica.

Les tres simulacions s'han realitzat amb èxit seguint tot el procés complet d'un atac de phishing. Per tant, s'han superat els imprevistos i dificultats. S'ha demostrat com es poden extreure dades personals de terceres persones mitjançant l'Enginyeria Social amb el propòsit de comprendre aquest atac més a fons per enfrontar aquesta amenaça de manera més eficient i ajudar en la defensa dels usuaris.

Després d'analitzar les respostes de l'enquesta a l'apèndix H, s'arriba a la conclusió que encara existeix un desconeixement massa alt en comparació amb la probabilitat de cada persona pugui rebre un cas de phishing i ser-ne víctima potencial. D'altra banda s'ha comprovat que el desconeixement no és absolut, si no que els aspectes principals o més comuns són coneguts per gran part de la mostra, tot i que de manera força superficial. Encara queda molt per aprendre respecte de les eines que utilitzem diàriament i les amenaces que aquestes poden comportar.

El món tendeix a digitalitzar-se tal i com s'està comprovant en els darrers anys, i ho fa a un ritme molt ràpid. Aquest fet implica que cada cop més persones seran usuàries de més tecnologies, les quals seran cada vegada més complexes. Conforme la tecnologia avança, també ho hauria de fer l'educació de la gent en aquest àmbit amb el propòsit de fer-ne un ús responsable i conscient. Cal donar a conèixer els perills als quals la gent està sotmesa i la facilitat amb la qual pot ser enganyada i estafada. D'aquí sorgeix la vessant més educativa d'aquest projecte.

6.2. Desenvolupament futur

Aquest projecte es podria seguir desenvolupant de diverses maneres, ja sigui ampliant-lo o complementant-lo.

Una opció que es va contemplar però que degut al temps no va poder ser possible és la realització d'una simulació de phishing real en un entorn determinat. Es podria crear un *email* de phishing i enviar-lo a un grup d'alumnes, ja sigui d'una assignatura, d'un curs o de qualsevol entorn controlat. El correu podria dirigir a una web la qual informés que s'ha estat víctima d'un phishing simulat. Addicional, que es presentés un document com el de l'apartat "3 Decàleg de bones pràctiques" de l'apèndix H amb mesures de detecció i prevenció d'aquest tipus d'atacs. No caldria demanar dades, ja que s'haurien d'emmascarar i demostrar que no s'està sostraient ni utilitzant tal informació. Aquestes pràctiques són comunes en empreses, on un departament realitza aquestes proves als empleats de la companyia.

Un altre cas seria augmentar la complexitat del *malware* de la simulació 3, enfocant el treball principalment en aquest tema i indicant que es troba en el marc contextual d'un atac de phishing. Hi hauria l'opció d'afegir codi maliciós a una eina ja creada, de manera que quan fos executada, l'usuari no veuria res estrany. No obstant, hi hauria actiu un procés secundari controlat per l'atacant. Per exemple, inserir codi a l'executable Putty de manera que pogués ser executat amb normalitat i alhora l'atacant tingués accés remot a l'equip de la víctima.

Un projecte que personalment considero molt interessant i que podria ser molt útil per a les persones seria la creació d'una eina antiphishing. Amb la informació facilitada referent a la detecció d'un phishing, es podria crear una aplicació que analitzés els correus electrònics i busqués indicis d'aquesta amenaça, atorgant-los una puntuació segons els resultats obtinguts. D'aquesta manera es podria adjudicar una valoració en funció de la probabilitat que el *email* fos part d'un atac de phishing.

Bibliografia

[1] "Hackear a las personas" *GMS*. [Online] Font: https://gmsseguridad.com/ing-social-info.html

[2] "Phishing" *Wikipedia*, 2018 *Wikipedia*. [Online] Font: https://es.wikipedia.org/wiki/Phishing

[3] "¿Qué es el phishing?" *Akamai*. [Online] Font: https://www.akamai.com/es/es/resources/what-is-phishing.jsp

[4] "Glosario de términos: ¿Qué es el Spear Phishing?" *S21SEC*, 2013. [Online] Font: https://www.s21sec.com/es/blog/2013/05/glosario-de-terminos-que-es-el-spear-phishing/

[5] "'Whaling', el nuevo fraude que amenaza a tu empresa" *Panda,* 2016. [Online] Font: https://www.pandasecurity.com/spain/mediacenter/seguridad/whaling-amenaza-contra-empresas/

[6] "10 consejos para evitar ataques de Phishing" *Panda*, 2016 [Online] Font: https://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/

[7] "Cómo conseguir contactos y bases de datos para campañas de email marketing y sms marketing." *Teenvio*, 2010. [Online] Font: https://www.teenvio.com/es/consejos/bases-de-datos-email-marketing/

[8] J. Pérez, M. Merino. "Definición de correo electrónico" *Deficinión.DE,* 2008. [Online] Font: https://definicion.de/correo-electronico/

[9] J.C. Villanueva. "Managed File Transfer and Network Solutions" *JSCAPE,* 2015. [Online] Font: https://www.jscape.com/blog/smtp-vs-imap-vs-pop3-difference

[10] "Simle Mail Transfer Protocol", *Wikipedia*, 2015. [Online] Font: https://ca.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

[11] "¿Qué es el Sender Policy Framewor o SPF en el email?" *Mittum*, 2016. [Online] Font: https://mittum.com/sender-policy-framework-email/

[12] "Claves para entender el concepto del DKIM (DomainKeys Identified Mail)" *Mittum*, 2017. [Online] Font: https://mittum.com/claves-dkim/

[13] "¿Qué es el DMARC y cómo debes implementarlo con el SPF y DKIM?" *Mittum*, 2017. [Online] Font: https://mittum.com/dmarc

[14] O. Long. "How Email Works (MTA, MDA, MUA)" *CCM,* 2018. [Online] Font: https://ccm.net/contents/116-how-email-works-mta-mda-mua

[15] *Simple Mail Transfer Protocol, Especificació.* IETF RFC 5321, Octubre 2008.

[16] *Internet Message Access Protocol, Especificació Versio 4.* IETF RFC 3501, Maig 2003

[17] *Post Office Protocol, Especificació Versió 3*. IETF RFC 1939, Maig 1996

[18] "Official Kali Linux Documentation". *Kali Linux*. [Online] Font: https://www.kali.org/kali-linux-documentation/

[19] "Web Phishing With Kali Linux (social engineering toolkit)" *Steemit,* 2018. [Online] Font: https://steemit.com/utopian-io/@rafiakbar366/web-phishing-with-kali-linux-social-engineering-toolkit

[20] "Phishing 101 using SocialFish Tool" *Latest Hacking News*, 2018- [Online] Font: https://latesthackingnews.com/2018/06/29/phishing-101-using-socialfish-tool/

[21] "Python", *Python*. [Online] Font: https://www.python.org

[22] "¿Qué es PHP?". *PHP*. [Online] Font: http://php.net/manual/es/intro-whatis.php

[23] M.S. Mariana Leguizamón, "EL PHISHING". M.S. Thesis, Grau en Sriminologia i Seguretat, Universitat Jaume I, Castellón de la Plana, Espanya.

[24] A.N.Belisario Méndez, "Análisis de Métodos de Ataques de Phishing". M.S.Thesis, Facultad de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería, Carrera de Especialización en Seguridad Informátiaca, Univetsidad de Buenos Aires, Buenos Aires, 2014, Argentina.

[25] X. Gombau Pascual, "Implementació d'un algoritme de detecció de phishing". M.S.Thesis, Escola Tècnica Superior d'Enginyeria de Telecomunicacions, Enginyeria de Tecnologies i Serveis de Telecomunicació menció en Telemàtica, Universitat Politècnica de Catalunya, 2018, Catalunya, Espanya.

[26] "Tipos MIME". *Mozilla*, 2018. [Online] Font: https://developer.mozilla.org/es/docs/Web/HTTP/Basics_of_HTTP/MIME_types

[27] "HTML". *Mozilla*, 2017. [Online] Font: https://developer.mozilla.org/es/docs/Web/HTML

[28] "Mensajes HTTP". *Mozilla*, 2018. [Online] Font: https://developer.mozilla.org/es/docs/Web/HTTP/Messages

[29] A. Guevara Benites. “Frontend y Backend”. *Devcode*. [Online] Font: https://devcode.la/blog/frontend-y-backend/

[30] “Apache HTTP server project”. *Apache.* [Online] Font: https://httpd.apache.org

[31] E. Sverdlov. “A Basic MySQL Tutorial”. *Digital Ocean*, 2012. [Online] Font: https://www.digitalocean.com/community/tutorials/a-basic-mysql-tutorial

[32] B. Bearnes. “¿Cómo instalar Linux, Apache, MySQL, PHP (LAMP) en Ubuntu 16.04?”. *Digital Ocean*, 2016. [Online] Font: https://www.digitalocean.com/community/tutorials/como-instalar-linux-apache-mysql-php-lamp-en-ubuntu-16-04-es

[33] “PHP mail() Function”. *w3schools*. [Online] Font: https://www.w3schools.com/php/func_mail_mail.asp

[34] “Msfvenom: la cosa va de payloads y encoders”. *Flu-project*, 2012. [Online] Font: https://www.flu-project.com/2012/08/msfvenom-la-cosa-va-de-payloads-y_28.html

[35] “¿Qué es un keylogger?”. *Kaspersky*. [Online] Font: https://latam.kaspersky.com/resource-center/definitions/keylogger

[36] S. González. “Estudio emailing: Evolución del email desde 1978 hasta hoy”. *Mailify*, 2016. [Online] Font: https://www.mailify.com/es/blog/email-marketing-2/evolucion-de-la-utilizacion-del-correo-electronico-con-el-paso-del-tiempo/

[37] E. Martinez Martinez. “El correo electrónico y su historia”. *Eveliux*, 2011. [Online] Font: http://www.eveliux.com/mx/El-correo-electronico-y-su-historia.html

[38] “Cabeceras de correo”. *Nerion*. [Online] Font: https://www.nerion.es/soporte/tutoriales/cabeceras-de-correo/

[39] “¿Cómo analizar las cabeceras de un correo normal?”. *Rincon del email*, 2014. [Online] Font: https://www.rincondelemail.es/analizar-las-cabeceras/

[40] “How does Email work?”. *Computer Networking Demystified*, 2014. [Online] Font: https://computernetworkingsimplified.wordpress.com/tag/smtp/

[41] “DMARC Overview”. *DMARC*. [Online] Font: https://dmarc.org/overview/

[42] Ki Nang Yip. “Whaling Case Study: Mattel's $3 Million Phishing Adventure”. *Infosec Insitute*. [Online] Font: https://resources.infosecinstitute.com/category/enterprise/phishing/spear-phishing-and-whaling/whaling-case-study/#gref

Glossari

Acrònim	Significat
CCO	Carbon Copy Occult (Còpia de Carbó Oculta). Camp de l'encapçalament d'un missatge de correu electrònic en el qual a diferència dels camps "Per a" o "CC", les adreces de correu romanen invisibles per als destinataris.
CSS	Cascading Style Sheets (Fulla d'estil en cascada). Llenguatge de disseny gràfic per definir i crear la presentació d'un document estructurant en un llenguatge de marcat.
DNS	Domain Name System. Sistema de nomenclatura jeràrquic descentralitzat per a dispositius connextat a xarxes IP com internet.
HTML	HyperText Markup Language. Llenguatge de marcat per a l'elaboració de pàgines web.
HTTPS	Hypertext Transfer Protocol Secure. Protocol d'aplicació basat en el protocol HTTP, destinat a la transferència segura de dades d'Hipertext.
LAMP	Linux Apache MySQL PHP. Sistema d'infraestructura de servidor web que fa servir les eines que formen l'acrònim.
MIME	Multipurpose Internet Mail Extensions. Conjunt de convencions o especificacions dirigides a l'intercanvi a través d'internet de tot tipus d'arxius de forma transparent per a l'usuari.
NAT	Network Address Translation. Mecanisme utilitzat pels routers IP per intercanviar paquets entre dues xarxes que assignen mútuament adreces incompatibles.
PHP	Hypertext Preprocessor. Llenguatge de programació utilitzat normalment a la banda del servidor originalment dissenyat per al desenvolupament web i contingut dinàmic.
SMS	Servei de Missatges Curts. Servei disponible en els telèfons mòbils que permet enviar i rebre missatges curts entre els seus usuaris.
SMTP	Simple Mail Transfer Protocol (protocol per transferència simple de correu). Protocol de xarxa utilitzat per l'intercanvi de missatges de correu electrònic.
SSL	Secure Socket Layer. Protocol criptogràfic que proporciona comunicacions segures per una xarxa, comunament internet.
TCP	Transmission Control Protocol. Un dels protocols fonamentals d'internet de la capa de transport OSI.
TLS	Transport Layer Security. Protocol criptogràfic que proporciona comunicacions segures per una xarxa, comunament internet. Millora del protocol SSL.
URL	Uniform Resource Locator. Identificador de recursos les adreces dels quals poden canviar, és a dir, que siguin variables.